

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

JESSE SACKIN, PETER HARRIS,
STEPHEN LUSTIGSON, NICHOLAS
MIUCCIO, and SARAH HENDERSON,
individually and on behalf of all others
similarly situated,

Plaintiff,

v.

TRANSPERFECT GLOBAL, INC.,

Defendant.

Case No. 17-cv-1469-LGS

**PLAINTIFFS' MEMORANDUM OF LAW IN OPPOSITION
TO DEFENDANT'S MOTION TO DISMISS THE AMENDED COMPLAINT
PURSUANT TO FEDERAL RULES OF CIVIL PROCEDURE 12(b)(1) AND 12(b)(6)**

TABLE OF CONTENTS

Table of Authorities.....	iii
Introduction.....	1
Factual Background.....	2
Argument.....	4
I. Plaintiffs Adequately Allege That They Sustained And Continue To Sustain Article III Injuries As A Result Of Defendant’s Unlawful Conduct.	4
A. Plaintiffs Need Only Plausibly Allege Injury For Article III Standing.	4
B. Plaintiffs Face An Imminent Risk Of Future Injury As A Result Of The Data Breach.	4
C. The Time And Expenses Plaintiffs Expended To Mitigate Harm Caused By Defendant’s Negligence Are Article III Injuries.	8
D. The Data Breach Diminished The Value Of Plaintiffs’ Personally Identifying Information.....	11
E. Plaintiffs Sustained Loss Of Privacy.	12
II. Plaintiffs Have Sufficiently Pled Their Claims For Relief.	13
A. Plaintiffs State A Claim For Negligence.	13
1. Defendant Owed A Duty Of Care To Plaintiffs.....	13
2. Plaintiffs Sustained Damages As A Result Of Defendant’s Breach Of Its Duty.	15
III. The Economic Loss Doctrine Does Not Apply To Plaintiffs’ Claims.....	16
B. Plaintiffs State A Claim For Breach Of Express Contract.....	16
1. Plaintiffs Adequately Allege The Existence Of Express Agreements.....	17

2.	Plaintiffs Adequately Allege Performance Pursuant To The Agreements.....	18
3.	Plaintiffs Adequately Allege Defendant's Breach Of The Agreements And Damage To Plaintiffs As A Result.	18
C.	Plaintiffs Allege A Breach Of Implied Contract.....	19
D.	Plaintiffs State A Claim For Unjust Enrichment.	21
E.	Plaintiffs State A Claim For Violation of N.Y. LABOR LAW § 203-d.....	22
CONCLUSION.....		25

TABLE OF AUTHORITIES**CASES**

<i>Ader v. Guzman</i> , 23 N.Y.S.3d 292 (N.Y. App. Div. 2016)	24, 25
<i>AHA Sales, Inc. v. Creative Bath Prod., Inc.</i> , 867 N.Y.S.2d 169 (2008)	23
<i>Alonso v. Blue Sky Resorts, LLC</i> , 179 F. Supp. 3d 857 (S.D. Ind. 2016)	8
<i>Anderson v. Hannaford Bros. Co.</i> , 659 F.3d 151 (1st Cir. 2011)	9
<i>Attias v. CareFirst, Inc.</i> , 199 F. Supp. 3d 193 (D.D.C. 2016)	8
<i>Beck v. McDonald</i> , 848 F.3d 262 (4th Cir. 2017).....	7
<i>Brian Hoxie’s Painting Co. v. Cato-Meridian Cent. School Dist.</i> , 76 N.Y.2d 207 (1990)	23
<i>Castillo v. Seagate Technologies, LLC</i> , No. 16-01958 (N.D. Cal. Sept. 14, 2016)	20
<i>Chu Chung v. New Silver Palace Restaurants, Inc.</i> , 272 F. Supp. 2d 314 (S.D.N.Y. 2003).....	23
<i>Clapper v. Amnesty Int’l USA</i> , 133 S. Ct. 1138 (2013)	4, 6, 8
<i>Claridge v. RockYou, Inc.</i> , 785 F. Supp. 2d 855 (N.D. Cal. 2011)	11
<i>Colorado Capital v. Owens</i> , 227 F.R.D. 181 (E.D.N.Y. 2005)	13
<i>Corona v. Sony Pictures Entertainment, Inc.</i> , 2015 WL 3916744 (N.D. Cal. June 15, 2015)	11, 14, 15
<i>Democratic Governors Ass’n v. Brandi</i> , No. 14-00544, 2014 WL 2589279 (D. Conn. June 10, 2014).....	8

<i>Dittman v. UPMC</i> , 154 A.3d 318 (Pa. Sup. Ct. 2017)	15
<i>Doe v. Chao</i> , 540 U.S. 614 (2004)	12
<i>Doe v. Roe</i> , 599 N.Y.S.2d 350 (1993)	24
<i>Duqum v. Scottrade, Inc.</i> , No. 15-1537, 2016 WL 3683001 (E.D. Mo. July 12, 2016)	8
<i>Enslin v. The Coca-Cola Co.</i> , 136 F. Supp. 3d 654 (E.D. Pa. 2015)	17, 18, 20, 21
<i>Eternity Global Master Fund Ltd. v. Morgan Guar. Trust Co. of N.Y.</i> , 375 F.3d 168 (2d Cir. 2004)	17
<i>Farash v. Cont'l Airlines, Inc.</i> , 574 F.Supp.2d 356 (S.D.N.Y. 2008)	13
<i>Fero v. Excellus Health Plan, Inc.</i> , No. 15-06569, 2017 WL 713660 (W.D.N.Y. Feb. 22, 2017)	12
<i>Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.</i> , 528 U.S. 167 (2000)	4
<i>Galaria v. Nationwide Mut. Ins. Co.</i> , 663 F. App'x 384 (6th Cir. 2016)	6, 7, 9, 10
<i>Georgia Malone & Co., Inc. v. Rieder</i> , 973 N.E.2d 743 (N.Y. 2012)	21
<i>Gerel Corp. v. Prime Eastside Holdings, LLC</i> , 783 N.Y.S.2d 355 (2004)	24
<i>German by German v. Fed. Home Loan Mortg. Corp.</i> , 896 F. Supp. 1385 (S.D.N.Y. 1995)	14
<i>Gorrill v. Icelandair/Flugleidir</i> , 761 F.2d 847 (2d Cir. 1985)	20
<i>Hammond v. The Bank of New York Mellon Corp.</i> , No. 08-6060, 2010 WL 2643307 (S.D.N.Y. June 25, 2010)	8, 21

<i>Harsco Corp. v. Segui</i> , 91 F.3d 337 (2d Cir. 1996).....	17
<i>Hedges v. Obama</i> , 724 F.3d 170 (2d Cir. 2013).....	8
<i>Henry v. Isaac</i> , 632 N.Y.S.2d 169 (1995).....	24, 25
<i>Holdings Ltd. Inv. Litig.</i> , 998 F. Supp. 2d 157 (S.D.N.Y. 2014).....	16
<i>Hydro Investors, Inc. v. Trafalgar Power Inc.</i> , 227 F.3d 8 (2d Cir. 2000).....	16
<i>In re Adobe Sys., Inc. Privacy Litig.</i> , 66 F. Supp. 3d 1197 (N.D. Cal. 2014)	5, 7
<i>In re Anthem, Inc. Data Breach Litigation</i> , No. 15- 02617, 2016 WL 3029783 (N.D. Cal. May 27, 2016)	12, 15
<i>In re Barnes & Noble Pin Pad Litig.</i> , No. 12-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013)	8
<i>In re Facebook Privacy Litigation</i> , 572 F. App'x 494 (9th Cir. 2014).....	11, 19
<i>In re Google Inc. Cookie Placement Consumer Privacy Litig.</i> , 806 F.3d 125 (3d Cir. 2015).....	12
<i>In re Hannaford Bros.</i> , 613 F.Supp.2d 108 (D. Me. 2009).....	15
<i>In re Horizon Healthcare Servs. Inc. Data Breach Litig.</i> , 846 F.3d 625 (3d Cir. 2017).....	12
<i>In re Nickelodeon Consumer Privacy Litig.</i> , 827 F.3d 262 (3d Cir. 2016).....	12
<i>In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.</i> , 45 F. Supp. 3d 14 (D.D.C. 2014)	7
<i>In re Sony Gaming Networks & Customer Data Sec. Breach Litig.</i> , 996 F. Supp. 2d 942 (S.D. Cal. 2014)	7

<i>In re SuperValu, Inc.,</i> No. 14-2586 ,2016 WL 81792 (D. Minn. Jan. 7, 2016).....	8
<i>In re Zappos,</i> 108 F. Supp. 3d 949 (D. Nev. 2015)	8
<i>John v. Whole Foods Mkt. Grp., Inc.,</i> 858 F.3d 732 (2d Cir. 2017).....	4
<i>Kenford Co., Inc. v. Erie County,</i> 67 N.Y.2d 257 (N.Y. Ct. App. 1986)	19
<i>Khan v. Children’s Nat’l Health Sys.,</i> 188 F. Supp. 3d 524 (D. Md. 2016)	7
<i>Krottner v. Starbucks Corp.,</i> 628 F.3d 1139 (9th Cir. 2010).....	5
<i>Leatherman v. Tarrant Cty. Narcotics Intelligence & Coordination Unit,</i> 507 U.S. 163 (1993)	17
<i>Leibowitz v. Cornell Univ.,</i> 584 F.3d 487 (2d Cir 2009)	19
<i>Lewert v. P.F. Chang’s China Bistro, Inc.,</i> 819 F.3d 963 (7th Cir. 2016).....	6, 9
<i>Longenecker-Wells v. Benecard Servs. Inc.,</i> 658 F. App’x 659 (3d Cir. 2016).....	21
<i>Lucatelli v. Texas de Brazil (Las Vegas) Corp.,</i> No. 11-1829, 2012 WL 1681394 (D. Nev. May 11, 2012).....	16
<i>Lujan v. Defenders of Wildlife,</i> 504 U.S. 555 (1992)	4
<i>Maas v. Cornell Univ.,</i> 94 N.Y.2d 87 (1999)	20
<i>Maimonides Medical Center v. First United American Life Ins. Co.,</i> 981 N.Y.S.2d 739 (N.Y. App. Div. 2014).....	23, 24
<i>Maraia v. Orange Reg’l Med. Ctr.,</i> 882 N.Y.S.2d 287 (2009)	24

<i>Martin v. Herzog</i> , 228 N.Y. 164 (1920)	14
<i>Moyer v. Michaels Stores, Inc.</i> , No. 14-561, 2014 WL 3511500 (N.D. Ill. July 14, 2014).....	5
<i>Nadel v. Play-By-Play Toys & Novelties, Inc.</i> , 208 F.3d 368 (2d Cir. 2000).....	20
<i>Nat’l Convention Servs., L.L.C. v. Applied Underwriters Captive Risk Assurance Co., Inc.</i> , No. 15-07063, 2017 WL 945189 (S.D.N.Y. Mar. 9, 2017)	25
<i>Palka v. Servicemaster Mgmt. Servs. Corp.</i> , 83 N.Y.2d 579 (1994)	13
<i>Peters v. St. Joseph Serv. Corp.</i> , 74 F. Supp. 3d 847 (S.D. Tex. 2015)	8, 19
<i>Pisciotta v. Old Nat’l Bancorp.</i> , 499 F.3d 629 (7th Cir. 2007).....	7
<i>Reilly v. Ceridian Corp.</i> , 664 F.3d 38 (3d Cir. 2011).....	8, 15, 19
<i>Remijas v. Neiman Marcus Group, LLC</i> , 794 F.3d 688 (7th Cir. 2015).....	5, 6, 9, 10
<i>Resnick v. AvMed, Inc.</i> , 693 F.3d 1317 (11th Cir. 2012).....	21
<i>Robert S. Nusinov, Inc. v. Principal Mut. Life Ins. Co.</i> , 80 F. Supp. 2d 101 (W.D.N.Y.)	20
<i>Roberts v. Univ. of Rochester</i> , 573 F. App’x 29 (2d Cir. 2014).....	13
<i>Ross v. AXA Equitable Life Ins. Co.</i> , No. 15-2665, 2017 WL 730266 (2d Cir. Feb. 23, 2017).....	8
<i>Ruiz v. Gap, Inc.</i> , 380 F. App’x 689 (9th Cir. 2010).....	7
<i>Ruiz v. Gap, Inc.</i> , 622 F. Supp. 2d 908 (N.D. Cal. 2009)	15

<i>Schwartz v. Torrenzano</i> , 16 N.Y.S.3d 697 (N.Y. Sup. Ct. 2015)	22, 24
<i>Spokeo v. Robins</i> , 136 S. Ct. 1540 (2016)	2, 4, 12
<i>Storm v. Paytime, Inc.</i> , 90 F. Supp. 3d 359 (W.D. Pa. 2015)	8
<i>Strautins v. Trustware Holdings, Inc.</i> , 27 F. Supp. 3d 871 n.11 (N.D. Ill. 2014)	8
<i>Svenson v. Google Inc.</i> , No. 13-04080, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015)	11, 12, 19
<i>Target Corp. Customer Data Sec. Breach Litig.</i> , 66 F. Supp. 3d 1154 (D. Minn. 2014)	20
<i>Travelers Cas. & Sur. Co. v. Dormitory Auth.-State of N.Y.</i> , 734 F. Supp. 2d 368 (S.D.N.Y. 2010)	16
<i>Uhr v. East Greenbush Cent. School Dist.</i> , 94 N.Y.2d 32 (1999)	25
<i>Walters v. Kimpton Hotel & Rest. Grp., LLC</i> , No. 16-05387, 2017 WL 1398660 (N.D. Cal. Apr. 13, 2017)	6, 15
<i>Whalen v. Michaels Stores</i> , 153 F. Supp. 3d 577 (E.D.N.Y. 2015)	7, 8, 9
<i>Worix v. MedAssets, Inc.</i> , 869 F. Supp. 2d 893 (N.D. Ill. 2012)	15

Statutes

N.Y. LABOR LAW § 203-d	passim
------------------------------	--------

Rules

Fed. R. Civ. P. 26(a)(1)	18
Fed. R. Civ. P. 8(d)(2)	22

Other Authorities

Restatement (Second) Torts § 652A (2016) 12

INTRODUCTION

Taking a stance that would shock its employees, Defendant TransPerfect Global, Inc. (“TransPerfect”) contends that it has no duty to take any precautions to protect the confidential personally identifiable information (“PII”) that its employees are required to provide as a condition of employment. This is no mere legal position adopted for this litigation; to the contrary, the fact that an employee was so easily duped into voluntarily sending the unencrypted Form W-2’s and payroll information of every TransPerfect employee speaks volumes as to Defendant’s negligent, if not non-existent, security precautions.

Defendant is wrong in asserting employers have no duty to protect PII. In addition to the common law duty of care, NEW YORK LABOR LAW § 203-d imposes an affirmative duty on employers not to disseminate PII like Social Security numbers. Defendant breached that duty by providing its employees’ Social Security numbers (and other PII) to criminals. Defendant has thus acted negligently in violation of a duty of care, just as it has breached its promise to safeguard its employees’ PII, and unjustly enriched itself at their expense.

Defendant is also wrong to suggest that Plaintiffs have not been injured by the dissemination of their PII to criminals. TransPerfect provided criminals with Plaintiffs’ most sensitive PII: names, addresses, banking information, and Social Security numbers. The complaint plausibly alleges that providing this information to criminals is injurious. After all, the reason the criminals wanted to obtain the W-2’s and payroll data was to commit identity theft and tax fraud. And, as the majority of U.S. Circuit Courts have held, the injuries attendant to data breaches, even those caused by the release of far less sensitive data than was provided here, confer Article III standing.

First, criminals can easily use Plaintiffs' Social Security numbers to commit identity theft and tax fraud, and the risk that this will occur is far more imminent than the risk associated with other data breaches in which courts found the risk of future harm was sufficient to create Article III standing. Second, Plaintiffs have been injured because they incurred expenses to mitigate the damages they reasonably anticipated after Defendant gave their PII to criminals. Third, Plaintiffs' PII is itself valuable, as demonstrated by the fact that criminals sell PII on the black market. The diminution of value in Plaintiffs' own identifying information is a cognizable injury. Fourth, Plaintiffs have sustained a loss of privacy as a result of the unauthorized disclosures -- an injury that has received near-universal recognition since the Supreme Court's decision in *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). Accordingly, Defendant's motion to dismiss should be denied.

FACTUAL BACKGROUND

On or around January 17, 2017, one or more TransPerfect employee received a phishing email purporting to be from TransPerfect's Chief Executive Officer requesting all of TransPerfect's current and former employees' 2015 Form W-2's and payroll data. Amended Complaint ("Complaint" or "Compl.") ¶¶ 14-16. Due to TransPerfect's failure to implement proper training, procedures, and controls regarding the handling of its employees' PII, at least one TransPerfect employee provided the requested information in an unencrypted format, disclosing, *inter alia*, names, addresses, detailed banking information, and Social Security numbers (the "Data Breach"). *Id.* ¶¶ 15, 31, 103, 104.¹

¹ Phishing scams, such as the one prompting the Data Breach in the instant case, are not uncommon, particularly during tax season. In fact, data security breaches have dominated the headlines over the past several years, with internet security experts warning of this precise scam intended to facilitate tax refund fraud. Compl. ¶¶ 24-26.

TransPerfect requires its employees to furnish their PII as a condition of their employment to verify identities, receive their pay, and for tax purposes. *Id.* ¶¶ 59, 74, 80. TransPerfect implicitly and explicitly promised that it would take adequate measures to protect PII, including standard data retention, encryption, and destruction policies. *Id.* ¶¶ 27-29, 60-63, 74, 80-85. These guarantees came in the forms of privacy policies, company security practices, TransPerfect's emphasis on data privacy and protection on its website, and implied duties attendant to the safeguarding of others' PII. *Id.*

Approximately a week after the Data Breach, TransPerfect began contacting its employees to inform them of the Data Breach and, recognizing that its employees faced the real risk of fraud and identity theft, encouraged employees to take concrete measures to protect themselves. *Id.* ¶¶ 8-12, 38. TransPerfect offered its employees up to two years of Experian's ProtectMyID, a markedly inferior service that fails to prevent identity theft from occurring and merely notifies its subscribers after-the-fact. *Id.* ¶¶ 37-40. In light of ProtectMyID's failure to provide any real protection, Plaintiffs were forced to purchase more useful identity theft protection services. *Id.* ¶¶ 8-12. Nor did TransPerfect offer compensation for the mitigation efforts it recommended to employees, which required, *inter alia*, consulting tax professionals, completing affidavits for federal and local tax officials, and scheduling and attending in-person meetings at the request of the IRS to verify their identities and tax returns. *Id.*

As a result of Defendant's negligence, Plaintiffs have incurred and will continue to incur damages in the form of, *inter alia*, attempted identity theft, time and expenses mitigating harms (*e.g.*, the costs of engaging and maintaining credit monitoring and protection services), increased risk of harm, diminished value of PII, and/or loss of privacy. *Id.* ¶ 34.

ARGUMENT

I. Plaintiffs Adequately Allege That They Sustained And Continue To Sustain Article III Injuries As A Result Of Defendant’s Unlawful Conduct.

A. Plaintiffs Need Only Plausibly Allege Injury For Article III Standing.

In order to satisfy Article III’s standing requirements, “a plaintiff must show (1) it has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000) (citing *Lujan*, 504 U.S. at 560). “At the pleading stage, general factual allegations of injury resulting from the defendant’s conduct may suffice . . .” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (quotation omitted). “Taking [the plaintiff’s] allegations as true and drawing all reasonable inferences in his favor,” the court need simply determine whether the plaintiff plausibly alleged an injury. *John v. Whole Foods Mkt. Grp., Inc.*, 858 F.3d 732 (2d Cir. 2017).

B. Plaintiffs Face An Imminent Risk Of Future Injury As A Result Of The Data Breach.

A plaintiff threatened with the possibility of future injury has standing when the threatened injury is “certainly impending” or “based on a ‘substantial risk’ that the harm will occur.” *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147, 1150 n.5 (2013) (emphasis and citations omitted). While there must be a “substantial risk” of harm, it need not be “literally certain” that the harms will materialize, as Defendant insists. *See id.* at 1150 n.5 (citation omitted); *see also Spokeo*, 136 S. Ct. at 1549 (“Article III standing requires a concrete injury . . . This does not mean, however, that the risk of real harm cannot satisfy that requirement.”).

Whereas in *Clapper*, “there was no evidence that any of respondents’ communications either had been or would be monitored,” TransPerfect’s employees’ PII was deliberately targeted by criminals and there is “no need to speculate as to whether [Plaintiffs’] information has been stolen and what information was taken.” *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 693 (7th Cir. 2015) (citation omitted).

Courts nationwide have thus consistently held that plaintiffs may demonstrate a substantial risk of future harm (*i.e.*, the increased risk of fraud or identity theft) by virtue of a data breach alone: “Why else would hackers break into a store’s database and steal consumers’ private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities.” *Remijas*, 794 F.3d at 693.²

As the Seventh Circuit explained, a plaintiff should not have to wait for actual misuse in order to confer standing, as “‘wait[ing] for the threatened harm to materialize in order to sue’ would create a different problem: ‘the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not ‘fairly traceable’ to the defendant’s data breach.’” *Remijas*, 794 F.3d at 693 (citing *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1215 n.5 (N.D. Cal. 2014); *cf. Moyer v. Michaels Stores, Inc.*, No. 14-561, 2014 WL 3511500, at *5 (N.D. Ill. July 14, 2014) (“If a bee’s anticipated pollination patterns create a sufficiently imminent risk of injury to alfalfa farmers who fear gene flow from genetically engineered plants in nearby fields, I fail to see how the transfer of information from a data hacker to an identity thief (assuming they are not one and the same) could be deemed an overly attenuated risk of harm.”) (citation omitted).

² *Accord Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1141-43 (9th Cir. 2010) (citation and emphasis omitted) (holding that employees whose PII was on a stolen laptop alleged “a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data,” despite the fact that there was no indication that the stolen PII had been fraudulently used).

In data breach cases involving hackers that intentionally target and steal PII, as was the case here, plaintiffs face a near certainty of impending injury because the “primary incentive” for hackers to steal data is to use it to commit identity theft or fraud. *See Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir. 2016). Numerous courts have therefore found that victims of targeted data breaches have Article III standing based on an imminent risk of harm, even where the stolen data had not yet been used.

Galaria v. Nationwide Mut. Ins. Co., 663 F. App’x 384, 388 (6th Cir. 2016) (unpublished) is on point. There, hackers breached an insurance and financial-services company’s computer systems and accessed its customers’ data including names, employers, and Social Security numbers. *Id.* at 386. Although it was not “literally certain” that misuse would occur, the plaintiffs’ allegations of a substantial risk of harm and reasonably incurred mitigation costs were sufficient to establish Article III standing because “[t]here is no need for speculation where Plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals.” *Id.* at 388.

Lewert is also instructive. *Lewert* involved a data breach of customer credit and debit card information. 819 F.3d at 965. The Seventh Circuit concluded that the plaintiffs’ future injury, namely the increased risk of fraudulent charges and identity theft, is concrete enough to provide standing because the “primary incentive” for hackers to steal data is to use it to make fraudulent charges or assume those customers’ identities. *Id.* at 967 (citing *Remijas*, 794 F.3d at 693). Courts throughout the country hold the same.³ Standing in this action is even stronger

³ *See Walters v. Kimpton Hotel & Rest. Grp., LLC*, No. 16-05387, 2017 WL 1398660, at *1 (N.D. Cal. Apr. 13, 2017) (“The Court respectfully disagrees that a plaintiff must actually suffer the misuse of his data or an unauthorized charge before he has an injury for standing purposes.”); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 962 (S.D. Cal. 2014) (notwithstanding *Clapper*, holding that “Plaintiffs’ allegations that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion [are] sufficient to establish Article III standing at this stage”); *In re Adobe Sys., Inc.*, 66 F. Supp. 3d at 1215 (“[T]o require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order

because here as opposed to credit and debit card numbers, the data obtained by the hackers included names, addresses, banking information, and Social Security numbers.

Defendant's reliance on the district court's decision in *Whalen v. Michaels Stores*, 153 F. Supp. 3d 577 (E.D.N.Y. 2015) is misplaced. In the subsequent appeal, the Second Circuit held that the plaintiff could not "plausibly face a threat of future fraud, because her stolen credit card was promptly canceled after the breach and no other personally identifying information -- such as her birth date or *Social Security number* -- is alleged to have been stolen." No. 16-260, 12017 WL 1556116, at *2 (2d Cir. May 2, 2017) (summary order) (emphasis added). The Court then proceeded to compare the facts in *Whalen* to those of *Galaria*, wherein the plaintiffs were found to have standing because the breached database contained information such as names, employers, and Social Security numbers. 12017 WL 1556116, at *2 n.1. The Second Circuit's opinion therefore supports the contention that where Social Security numbers are implicated in a data breach, as is the case here, the risk of future harm is sufficient to confer standing.⁴

to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact."); *Ruiz v. Gap, Inc.*, 380 F. App'x 689, 691 (9th Cir. 2010) (unpublished) (holding at summary judgment stage that the plaintiff's "alleged prospective injury [greater risk of identity theft following the theft of a laptop containing his PII] presents enough of a risk that the concerns of plaintiffs are real, and not merely speculative. Ruiz has sufficient Article III standing to pursue his claims."); *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 634 (7th Cir. 2007) (holding that plaintiffs whose data had been stolen but not yet fraudulently used suffered an injury-in-fact); *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524 (D. Md. 2016) ("[P]laintiffs have properly alleged an injury in fact arising from increased risk of identity theft if they put forth facts that provide . . . a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud.").

⁴ The other authorities upon which Defendant relies are also inapposite. Three involve stolen hardware storing PII like laptops which were stolen not for the PII but for the hardware itself, thus making a claim that the PII would be accessed and misused mere speculation. See *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) ("[E]ven after extensive discovery, the *Beck* plaintiffs have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information[.]"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 20-25 (D.D.C. 2014) (where a criminal broke into a car and stole the car's GPS, stereo, and tapes which contained PII, the court found that the chain of events too speculative because the thief would have to recognize the tapes as data tapes, obtain special equipment to read the tapes, break the encryption, acquire software to upload the tapes to a computer, understand the database, and then misuse or sell the data); *Hammond v. The Bank of New York Mellon Corp.*, No. 08-6060, 2010 WL 2644407 (S.D.N.Y. June 25, 2010) (holding that where metal boxes containing tapes storing PII were lost from two trucks, it was likely that the boxes

C. The Time And Expenses Plaintiffs Expended To Mitigate Harm Caused By Defendant's Negligence Are Article III Injuries.

The costs Plaintiffs incurred and will continue to incur indefinitely are concrete injuries suffered in reasonable efforts to mitigate imminent harms. *See Democratic Governors Ass'n v. Brandi*, No. 14-00544, 2014 WL 2589279, at *7 (D. Conn. June 10, 2014) (holding “where there is a ‘substantial risk’ that a harm will occur, prompting a plaintiff to reasonably incur costs to mitigate or avoid that harm, standing may be found.”) (citing *Clapper*, 133 S. Ct. at 1150 n.5; *Hedges v. Obama*, 724 F.3d 170, 195-96 (2d Cir. 2013)).

A number of Circuit Courts have held that mitigation expenses following a data breach constitute Article III injuries. *See Lewert*, 819 F.3d at 967-68 (“[B]ecause their data has already been stolen,” Plaintiffs’ harm was imminent and their mitigation expenses, *e.g.*, purchasing

were actually lost and never accessed, or that the thieves stole the metal boxes hoping they contained money rather than with the intent to steal PII). Other cases are inapposite because the data stolen did not include Social Security numbers and was not sensitive in nature or the harm could be remedied with relative ease, *i.e.*, by cancelling a credit card. *See Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193, 197 (D.D.C. 2016) (stolen information merely consisted of names, birth dates, email addresses, and subscriber identification numbers); *In re SuperValu, Inc.*, No. 14-2586, 2016 WL 81792, at *1 (D. Minn. Jan. 7, 2016) (disclosing cardholder names, account numbers, expiration dates, and PINs); *Alonso v. Blue Sky Resorts, LLC*, 179 F. Supp. 3d 857, 879 (S.D. Ind. 2016) (hackers obtained only “names, credit card numbers, and card expiration dates”); *Whalen*, 153 F. Supp. 3d at 578 (hackers only retrieved easily changeable basic credit and debit card information); *In re Zappos*, 108 F. Supp. 3d 949 (D. Nev. 2015) (revealing only names, addresses, passwords, and last four digits of credit and debit cards); *In re Barnes & Noble Pin Pad Litig.*, No. 12-8617, 2013 WL 4759588, at *4 (N.D. Ill. Sept. 3, 2013) (involving only credit and debit card numbers and PINs, and “there are no facts alleged to support the conclusion Plaintiffs’ information was disclosed”). Defendant also improperly relies upon cases where it is unclear whether the data had been stolen or where the PII was stolen for unrelated purposes. *See Reilly v. Ceridian Corp.*, 664 F.3d 38, 40, 46 (3d Cir. 2011) (“It is not known whether the hacker read, copied, or understood the data” and there was no evidence of any misuse); *Duqum v. Scottrade, Inc.*, No. 15-1537, 2016 WL 3683001, at *4 (E.D. Mo. July 12, 2016) (holding that where hackers obtained data for stock price manipulation scheme, there was no reason to suggest hackers intended to commit identity theft or fraud); *Strautins v. Trustware Holdings, Inc.*, 27 F. Supp. 3d 871, at *4, *5 n.11 (N.D. Ill. 2014) (holding that the plaintiff could not prove that her information had been stolen). Defendant also cites to *Ross v. AXA Equitable Life Ins. Co.*, No. 15-2665, 2017 WL 730266 (2d Cir. Feb. 23, 2017), which is not a data breach action and where the plaintiffs relied on a highly speculative chain of events which included, *inter alia*, an economic downturn in order to allege that the insurer-defendant’s purported misrepresentations create an increased risk of nonpayment of insurance obligations in the future. Moreover, many of Defendant’s cases have been effectively invalidated by the Supreme Court’s decision in *Spokeo*, which, as discussed at length *infra* Section I.E., has been interpreted by Circuit Court decisions such as *Google*, *Nickelodeon*, and *Horizon* as recognizing an intrusion or loss of privacy, as well as an increased risk of harm, as cognizable injuries. *See, e.g., Reilly*, 664 F.3d 38 (dismissed for lack of injury); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359 (W.D. Pa. 2015) (same); *Peters v. St. Joseph Serv. Corp.*, 74 F. Supp. 3d 847 (S.D. Tex. 2015) (same).

credit monitoring, and time and effort monitoring financial statements, qualify as “actual injuries”); *Galaria*, 663 F. App’x at 388 (mitigation expenses, including the time and money spent monitoring bank statements and credit, are reasonable, concrete injuries); *Remijas*, 794 F.3d at 694 (“[H]aving been notified by Neiman Marcus that her card is at risk,” purchasing credit monitoring was a reasonable mitigation expense and a concrete injury); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 165-66 (1st Cir. 2011) (mitigation expenses “reasonable” where there was a “deliberate taking of credit and debit card information by sophisticated thieves.”). Defendant asserts that these decisions were improperly decided. Not so.

In fact, the Second Circuit’s recent opinion in *Whalen v. Michaels Stores, Inc.* intimates that the Second Circuit would follow *Remijas* and *Lewert* if presented with facts similar to the case at bar. 12017 WL 1556116, at *2 n.1. While the Court ultimately dismissed Whalen’s mitigation allegation, the decision distinguished *Remijas* and *Lewert* because Whalen “pleaded no specifics about any time or effort that she [] spent monitoring her credit” and only alleged that “consumers must expend considerable time” monitoring credit. *Id.* Here, Plaintiffs plead those facts in spades. Compl. ¶¶ 8-12, 37. As such, the Second Circuit’s rationale for dismissing Whalen’s claim is absent here and its citation with approval to *Remijas* and *Lewert* is telling.

This is not a case where Plaintiffs seek to “manufacture standing by incurring costs in anticipation of non-imminent harm,” as Defendant suggests. *See id.* at 1155. Rather, expenditures taken to prevent or mitigate harms caused by others are not only cognizable, but are required under common law. “[I]t would be unreasonable to expect Plaintiffs to wait for actual misuse -- a fraudulent charge on a credit card, for example -- before taking steps to ensure their own personal and financial security, particularly when [the Defendant] recommended taking these steps.” *Galaria*, 663 F. App’x at 388. Indeed, the disclosures in the instant case, which

implicate names, addresses, Social Security numbers, and banking information, will likely be used in a manner with far more long-term and consequential effects than credit card information which can promptly be cancelled, thereby making mitigation even more necessary. Compl. ¶¶ 14, 16.

Given the gravity of the Breach, Plaintiffs have had to continuously monitor their credit and financial accounts, meet with tax professionals, schedule and attend in-person meetings at the request of the IRS to verify their identities and tax returns (which required taking time off from work for at least one Plaintiff), and spend time procuring extra security measures for their tax returns (*e.g.*, filing Form 14039's and/or requesting Identity Protection PINs). Compl. ¶¶ 8-12, 34, 38. The reality of risk and necessity of mitigation is further amplified by Defendant's own (albeit inadequate) response. It is telling that Defendant offered all of its effected Employees two years of credit monitoring and identity theft protection, and encouraged its victims to take IRS-recommended precautions when filing their tax returns. "It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded." *Remijas*, 794 F.3d at 694. Furthermore, that Defendant argues that the time and expenses Plaintiffs incurred safeguarding their tax returns are "manufactured" injuries when TransPerfect encouraged its employees take these precautions following the Breach is not well taken. This is especially so given that TransPerfect offered Plaintiffs enrollment in Experian's ProtectMyID Elite, which provides after the fact alerts, but no actual protection to prevent identity theft. *See* Compl. ¶¶ 37-39. TransPerfect's decision to provide inadequate protection only highlights the necessity of Plaintiffs purchasing more viable credit protection services to protect themselves.

**D. The Data Breach Diminished
The Value Of Plaintiffs’ Personally Identifying Information.**

Plaintiffs suffered a diminution of the value of their PII as a result of Defendant’s negligence. PII is a valuable commodity, and because Plaintiffs’ PII is now in the hands of criminals and Plaintiffs lost control over its dissemination, Plaintiffs’ PII is less valuable. Compl. ¶¶ 31, 35. Several courts persuasively hold that the loss of value in one’s PII is a cognizable injury. In *In re Facebook Privacy Litigation*, 572 F. App’x 494, 494 (9th Cir. 2014) (unpublished), plaintiffs contended that “they were harmed both by the dissemination of their personal information and by losing the sales value of that information.” The court concluded that such “allegations [were] sufficient to show the element of damages for [plaintiffs’] breach of contract and fraud claims.” *Id.* The court in *Svenson v. Google Inc.*, No. 13-04080, 2015 WL 1503429, at *2, *4 (N.D. Cal. Apr. 1, 2015) likewise found that “allegations of diminution in value of her personal information are sufficient to show contract damages for pleading purposes.”⁵ As Judge Koh held:

[T]he SAC does aver that Plaintiffs’ PII “is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.” . . . These allegations could be read to infer that an economic market existed for Plaintiffs’ PII, and that the value of Plaintiffs’ PII decreased as a result of the Anthem data breach. . . Plaintiffs are not required to plead that there was a market for their PII and that they somehow also intended to sell their own PII.

In re Anthem, Inc. Data Breach Litigation, No. 15- 02617, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016).⁶

⁵ *Accord Corona v. Sony Pictures Entertainment, Inc.*, 2015 WL 3916744, at *3 (N.D. Cal. June 15, 2015) (holding that the plaintiffs had sufficiently pleaded economic injury by claiming “that the[ir] PII was stolen and posted on file-sharing websites for identity thieves to download.”); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 865 (N.D. Cal. 2011) (finding plaintiff alleged standing and injury where “the breach of his PII has caused him to lose some ascertainable but unidentified ‘value’ and/or property right inherent in the PII.”).

⁶ Defendant relies on *Fero v. Excellus Health Plan, Inc.*, No. 15-06569, 2017 WL 713660 (W.D.N.Y. Feb. 22, 2017) to suggest that that Plaintiffs failed to allege how their personal information was made less valuable following the

E. Plaintiffs Sustained Loss Of Privacy.

The Supreme Court and Circuit Courts have held that the loss of privacy qualifies as an injury-in-fact for the purposes of Article III. *See, e.g., Doe v. Chao*, 540 U.S. 614, 641 (2004) (finding that the plaintiff had Article III standing based on allegations that he was “greatly concerned and worried” by the disclosure of his Social Security number and its potential consequences); *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 638 (3d Cir. 2017) (holding that “unauthorized *disclosures* of information have long been seen as injurious” and citing Restatement (Second) Torts § 652A (2016) for the proposition that “[o]ne who invades the right of privacy of another is subject to liability for the resulting harm to the interest of the other”) (internal quotations and citations omitted).⁷ New York recognizes a right to privacy over personal information, and does so for employees for the precise information disclosed here in LABOR LAW § 203-d. Consequently, by virtue of Defendant’s failure to secure and non-consensual disclosure of Plaintiffs’ PII to unknown cybercriminals, Plaintiffs suffered and continue suffer a loss of privacy sufficient to confer standing.

Data Breach, or how the Breach made their personal information less valuable. Judge Koh persuasively rejected this argument when she held that it is sufficient for plaintiffs to allege that there is a market for their PII, an allegation that Plaintiffs’ make here. *See In re Anthem*, 2016 WL 3029783, at *15; Compl. ¶¶ 31-35. The *Svenson* Court also rejected the notion that a plaintiff must plead with specificity exactly how their PII has been diminished in value or how a plaintiff might have profited from its sale. *Svenson*, 2015 WL 1503429, at *5.

⁷ *See also In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 273 (3d Cir. 2016), *cert. denied sub nom. C. A. F. v. Viacom Inc.*, 137 S. Ct. 624 (2017) (holding that the defendant’s disclosure of information relating to the plaintiffs’ online behavior was a clear *de facto* injury for Article III purposes); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 134 (3d Cir. 2015), *cert. denied sub nom. Gourley v. Google, Inc.*, 137 S. Ct. 36 (2016) (holding that the invasion and loss of privacy arising out of tracking and disclosure of users’ online behavior without consent satisfied federal standing requirements); *cf. Spokeo*, 136 S. Ct. at 1549 (“Although tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.”).

II. Plaintiffs Have Sufficiently Pled Their Claims For Relief.

A. Plaintiffs State A Claim For Negligence.

Under New York law, a plaintiff asserting negligence must allege: “(1) the existence of a duty on defendant’s part as to plaintiff; (2) a breach of this duty; and (3) injury to the plaintiff as a result thereof.” *Farash v. Cont’l Airlines, Inc.*, 574 F.Supp.2d 356, 367 (S.D.N.Y. 2008) (quotation omitted). Plaintiffs have done so here.

1. Defendant Owed A Duty Of Care To Plaintiffs.

There are two sources of the duty of care Defendant owed Plaintiffs to safeguard their PII. Not only does that duty arise under the common law, but N.Y. LABOR LAW 203-d specifically creates a duty on employers not to disseminate PII like Social Security numbers. Thus, Defendant’s contention that it need make no effort to protect its employees’ PII falls flat.

Whether a defendant owed a common law duty of care to a plaintiff is a threshold legal question for the Court. Courts “fix the duty point by balancing factors, including the reasonable expectations of parties and society generally, the proliferation of claims, the likelihood of unlimited or insurer-like liability, disproportionate risk and reparation allocation, and public policies affecting the expansion or limitation of new channels of liability.” *Palka v. Servicemaster Mgmt. Servs. Corp.*, 83 N.Y.2d 579, 586 (1994) (finding employer owed employee duty of care); *accord Roberts v. Univ. of Rochester*, 573 F. App’x 29, 31-33 (2d Cir. 2014) (summary order) (reversing trial court’s finding that no duty of care existed).⁸ Here, each of the factors favor finding a duty exists. Both Defendant’s employees and society in general expect that employers will protect the PII employees provide as a condition of employment. Nor should the Court be concerned about a proliferation of claims or the expansion of new channels

⁸ Unlike an action for breach of fiduciary duty, “[n]o such ‘special relationship’ is required to establish a duty of reasonable care in a negligence action.” *Colorado Capital v. Owens*, 227 F.R.D. 181, 189 (E.D.N.Y. 2005).

of liability, as the duty is limited to the employee-employer relationship. There is no disproportionate risk and reparation allocation, as employees have no control over the risk to the safety of their PII, whereas employers have the resources to protect PII and the control to do so.

Furthermore, under New York law, a statute or regulation establishes a standard of conduct such that its violation becomes negligence *per se* when the plaintiff is within the class of persons the statute or regulation is intended to protect against the harms suffered. *See German by German v. Fed. Home Loan Mortg. Corp.*, 896 F. Supp. 1385, 1396 (S.D.N.Y. 1995) (“Under the rule of negligence *per se*, if a statute is designed to protect a class of persons, in which the plaintiff is included, from the type of harm which in fact occurred as a result of its violation, the issues of the defendant's duty of care to the plaintiff and the defendant's breach of that duty are conclusively established upon proof that the statute was violated.”) (citing *Martin v. Herzog*, 228 N.Y. 164 (1920)). Here, N.Y. LABOR LAW § 203-d imposes a duty upon employers to protect their employees’ PII. Defendant has not contested that it violated N.Y. LABOR LAW § 203-d. Consequently, Plaintiffs have adequately alleged that they are within the class of persons the statute protects, and that the harm suffered is the kind the statute was designed to protect against.

Under circumstances similar to the instant action, courts have determined that plaintiffs adequately stated claims for negligence. *See, e.g., Corona v. Sony Pictures Entertainment, Inc.*, 2015 WL 3916744, at *3-5 (N.D. Cal. June 15, 2015) (holding that employees plausibly alleged negligence as a result of Sony’s data breach). Moreover, unlike traditional breaches where third parties enter into a victim’s system and take the information they seek, there was no such third party intrusion and taking in the instant case; rather, Defendant affirmatively and wrongfully disclosed Plaintiffs’ PII to third-party cybercriminals.⁹

⁹ The cases Defendant cites are distinguishable in that they are not in the context of employer-employee relationships or apply foreign state common law. *See, e.g., Worix v. MedAssets, Inc.*, 869 F. Supp. 2d 893 (N.D. Ill.

**2. Plaintiffs Sustained Damages
As A Result Of Defendant's Breach Of Its Duty.**

Defendant argues that Plaintiffs do not allege that they have suffered any “actual cognizable injury.” But Plaintiffs have plausibly alleged actual damages in the forms of, *inter alia*, increased risk of harm, diminished value of their PII, loss of privacy, purchasing and indefinitely maintaining credit and identity monitoring services, and -- at least in part *at Defendant's recommendation* -- spending time remedying or mitigating harms as a result of the Breach. Compl. ¶ 37. These injuries are cognizable. *See, e.g., Walters*, 2017 WL 1398660, at *2 (“Walters sufficiently alleged ‘actual damages’ flowing from the alleged breach, including having to ‘secure and maintain’ credit monitoring services (which presumably come at a cost) and other ‘out-of-pocket expenses and the value of . . . time reasonably incurred to remedy or mitigate’ the breach.”); *Corona*, 2015 WL 3916744, at *3-5 (“Plaintiffs adequately allege a cognizable injury by way of costs relating to credit monitoring, identity theft protection, and penalties.”); *cf. Anthem*, 2016 WL 3029783, at *16 (holding that the plaintiffs sufficiently pleaded “appreciable and actual” damages for benefit of the bargain losses, loss of value of PII, and mitigation expenses in connection with breach of contract claims).¹⁰

2012); *Dittman v. UPMC*, 154 A.3d 318, 325 (Pa. Sup. Ct. 2017). Defendant also inappropriately raises a line of cases regarding third party criminality that do not apply to the facts of this case.

¹⁰ The cases Defendant cites are not instructive because there was no imminent risk of harm. *See, e.g., Reilly*, 664 F.3d at 46 (holding that harm was too speculative to merit mitigation expenses because “[i]t is not known whether the hacker read, copied, or understood the data”); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 914 (N.D. Cal. 2009) (“Ruiz presents no evidence showing there was an actual exposure of his personal information[.]”). Defendant’s reliance on the district court’s decision in *In re Hannaford Bros.*, 613 F.Supp.2d 108 (D. Me. 2009) for the proposition that the court “dismiss[ed] plaintiffs’ claims where they failed to allege improper charges had not been reimbursed,” Defendant’s Motion to Dismiss (“Def.’s Mtn.”) 13, is particularly surprising considering that the proposition was overturned on appeal. *Anderson*, 659 F.3d at 162-67 (“[R]evers[ing] the district court’s dismissal of the plaintiffs’ negligence and implied contract claims as to [mitigation] damages.”).

III. The Economic Loss Doctrine Does Not Apply To Plaintiffs' Claims.

Defendant cites the general rule that purely economic loss cannot be recovered on a negligence claim. But, “[t]he New York Court of Appeals has admonished [] that the ‘economic loss rule’ should not be used outside of the product-liability context, and that a ‘duty’-based analysis should be applied instead.” *Travelers Cas. & Sur. Co. v. Dormitory Auth.-State of N.Y.*, 734 F. Supp. 2d 368, 378 (S.D.N.Y. 2010) (citation omitted). As noted above, Defendant had a duty to Plaintiffs here.

Moreover, the economic loss doctrine does not apply if a plaintiff can show that the legal duty underlying the tort claim is separate and apart from the contract claim. *See, e.g., Hydro Investors, Inc. v. Trafalgar Power Inc.*, 227 F.3d 8, 18 (2d Cir. 2000) (“[T]he rule allows such recovery in . . . cases involving liability for the violation of a professional duty.”). Here, Plaintiffs’ negligence claim is grounded in part on Defendant’s violation of N.Y. LABOR LAW § 203-d, which imposes duties that are separate from any contractual obligations. *See, e.g., In re MF Glob. Holdings Ltd. Inv. Litig.*, 998 F. Supp. 2d 157, 185 (S.D.N.Y. 2014), *aff’d*, 611 F. App’x 34 (2d Cir. 2015) (economic loss doctrine does not apply where “Regulations created a separate legal duty owed by [the defendant to the plaintiff] apart from any contract . . .”); *Lucatelli v. Texas de Brazil (Las Vegas) Corp.*, No. 11-1829, 2012 WL 1681394, at *5 (D. Nev. May 11, 2012) (where duty “arises from statutory, not contractual, obligations,” plaintiff’s loss is not “purely economic” and economic loss rule is inapplicable).

B. Plaintiffs State A Claim For Breach Of Express Contract.

To plead a claim for breach of contract under New York law, a plaintiff must show “(1) the existence of an agreement, (2) adequate performance of the contract by the plaintiff, (3) breach of contract by the defendant, and (4) damages.” *Eternity Global Master Fund Ltd. v.*

Morgan Guar. Trust Co. of N.Y., 375 F.3d 168, 177 (2d Cir. 2004) (reversing dismissal of breach of contract claim).

1. Plaintiffs Adequately Allege The Existence Of Express Agreements.

Plaintiffs adequately allege the existence of express agreements. *See* Compl. ¶ 74. Plaintiffs also allege the essential terms of the agreements. *Id.* (“The employment agreements involved a mutual exchange of consideration whereby TransPerfect entrusted Plaintiffs and Class Members with particular job duties and responsibilities in furtherance of TransPerfect’s services, in exchange for the promise of employment, with salary, benefits, and secure PII.”). Defendant’s assertion that Plaintiffs’ claim fails for want of allegations of “any provisions of their employment agreements that address data security,” Def.’s Mtn. 15, is without merit. Plaintiffs need not quote specific contract provisions that address this breach in order to plead their claim. *See Leatherman v. Tarrant Cty. Narcotics Intelligence & Coordination Unit*, 507 U.S. 163, 168 (1993) (“Rule 8(a)(2) requires that a complaint include only “a short and plain statement of the claim showing that the pleader is entitled to relief.”); *Harsco Corp. v. Segui*, 91 F.3d 337, 348 (2d Cir. 1996) (citing *Leatherman* and noting the district court’s dismissal because plaintiff failed to allege the specific representation or warranty breached, “may have applied an overly strict pleading standard to [the plaintiff’s] breach of contract claim”).

Indeed, in *Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654 (E.D. Pa. 2015), the court considered materially identical allegations and denied the defendants’ motion to dismiss the plaintiff’s claim for breach of contract. In *Enslin*, neither party -- either in the complaint or the briefing on the motion to dismiss -- ever specified particular contractual language or proffered an applicable employment agreement for consideration by the court. *See Enslin v. The Coca-Cola Co.*, No. 14-6476, ECF. Nos. 1 (complaint), 10 (motion to dismiss), 16 (opposition), & 19

(reply). Nevertheless, the court found that the plaintiff's allegations "[were] sufficient to support the existence of a contract, as well as its essential terms." 136 F. Supp. 3d at 675 (denying motion to dismiss claim for breach of contract where the plaintiff alleged a "mutual exchange of consideration whereby the [defendants] entrusted [the plaintiff] . . . with access to the vehicles and equipment for the sale of one of America's most secure brands, Coca-Cola, in exchange for the promise of employment, with salary, benefits, and secure PII").¹¹

2. Plaintiffs Adequately Allege Performance Pursuant To The Agreements.

Defendant's assertion that Plaintiffs have failed to allege performance pursuant to the agreement, *see* Def.'s Mtn. 15-16, is without merit. Defendant's argument rests on the faulty premise that "Plaintiffs performed their job duties in exchange for a promise of compensation, not for security measures." *Id.* at 16. However, Plaintiffs have, as noted *supra.*, adequately alleged that the material terms of the agreement with Defendant included the requirement that Defendant secures Plaintiffs' and Class Members' PII.

3. Plaintiffs Adequately Allege Defendant's Breach Of The Agreements And Damage To Plaintiffs As A Result.

Plaintiffs allege (and Defendant does not contest) that Defendant breached its obligation to protect Plaintiffs' and Class Members' PII. *See* Compl. ¶¶ 14-17 (describing breach) & ¶ 75 ("TransPerfect's failure to protect Plaintiffs' and Class Members' PII constitutes a material breach of the terms of the agreement by TransPerfect.").

¹¹ Indeed, Defendant was obliged, pursuant to this Court's June 15, 2017 scheduling order, to provide initial disclosures pursuant to Fed. R. Civ. P. 26(a)(1) by June 20, 2017, and to proceed with discovery "on the individual claims pending resolution of Defendant's motion to dismiss the Amended Complaint." *See* ECF. No. 25. To date, Defendant has done neither, choosing instead to ignore its obligations to provide initial disclosures and to seek extensions to its deadlines to provide discovery responses relating to the Plaintiffs (a mere five individuals). Accordingly, Defendant should not be heard to argue that Plaintiffs have failed to state a claim due to Plaintiffs' inability to proffer the agreements or specify the exact language underlying their claims for breach of express contract.

Plaintiffs also allege actual damages as a result of Defendant's breach. *See e.g.*, Compl. ¶¶ 34, 77. Indeed, Plaintiffs' "allegations of diminution in value of [their] personal information are sufficient to show contract damages for pleading purposes." *Svenson*, 2015 WL 1503429, at *5 (denying dismissal of breach of contract claim based on data breach involving PII, citing *In re Facebook*, 572 Fed. Appx. 494).

Accordingly, Defendant's assertion that Plaintiffs fail to allege actual damages is without merit, and Defendant's cited authority is inapposite.¹²

C. Plaintiffs Allege A Breach Of Implied Contract.

A cause of action for breach of implied contract requires the same elements as a cause of action for breach of contract. *Leibowitz v. Cornell Univ.*, 584 F.3d 487, 506-507 (2d Cir 2009). Here, Plaintiffs adequately allege the existence of an implied contract. Indeed, Plaintiffs identify the consideration and material terms of the agreement. *See* Compl. ¶¶ 27-29, 80-81. And Defendant does not dispute the nature of this agreement, that the parties had legal capacity to enter such an agreement, or that such an agreement would be legal.

Plaintiffs also adequately allege mutual assent to be bound, and Defendant's assertion to the contrary, Def.'s Mtn. 16-18, is without merit. Although an implied-in-fact contract must have mutual assent, such assent can be inferred from "the specific conduct of the parties, industry custom, and course of dealing." *Nadel v. Play-By-Play Toys & Novelties, Inc.*, 208 F.3d 368, 376 & n.5 (2d Cir. 2000) (citing *Maas v. Cornell Univ.*, 94 N.Y.2d 87, 94 (1999)).

Moreover, an implied employment contract can be inferred from the contents of an intra-

¹² In *Reilly*, unlike here, "[i]t [was] not known whether the hacker read, copied, or understood the data." 664 F.3d at 40. In *Peters*, 74 F. Supp. 3d 847, unlike here, the district court only addressed whether the allegations supported a finding of injury under plaintiff's federal statutory claims. *See id.* at 852. Here, in contrast, Plaintiffs allege claims *solely* based on state or common law. *Kenford Co., Inc. v. Erie County*, 67 N.Y.2d 257 (N.Y. Ct. App. 1986), unlike here, involved a claim for the "[l]oss of future profits as damages for breach of contract." *Id.* at 261.

corporate document and the parties' behavior with respect thereto. *See, e.g., Gorrill v. Icelandair/Flugleidir*, 761 F.2d 847, 852 (2d Cir. 1985) (binding implied contract based on the terms of an internal operations manual and the actions of the parties in relation thereto).

Here, Plaintiffs allege conduct by the parties and a course of dealing from which mutual assent can be reasonably inferred. *See* Compl. ¶¶ 27-29. Such allegations provide adequate factual support for the existence of an implicit agreement by Defendant that it would take adequate measures to protect Plaintiffs' and Class Members' PII. *See e.g., Enslin*, 136 F. Supp. 3d at 675 (denying motion to dismiss breach of implied contract where the plaintiff pled that the defendant, "through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard his PII in exchange for his employment"); *Castillo v. Seagate Technologies, LLC*, No. 16-01958, ECF. No. 39, at 17 (N.D. Cal. Sept. 14, 2016) ("While Seagate made no explicit promises as to the ongoing protection of personal information, it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently.") (citing *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014)), Ex. 1 to Declaration of Jeremiah Frei-Pearson ("Frei-Pearson Decl.")).¹³

¹³ Defendant offers no factual support for its argument that there was no mutual intent by the parties, and Defendant's cited authority are inapposite. In *Robert S. Nusinov, Inc. v. Principal Mut. Life Ins. Co.*, 80 F. Supp. 2d 101 (W.D.N.Y.), unlike here, there was a written agreement at odds with the alleged implied contract. *See* 80 F. Supp. 2d at 107. And in *Longenecker-Wells v. Benecard Servs. Inc.*, 658 F. App'x 659 (3d Cir. 2016) (unpublished), the court dismissed the breach of implied contract claim because the plaintiffs, unlike here and in *Enslin*, failed to plead "any company-specific documents or policies from which one could infer an implied contractual duty to protect Plaintiffs' information." 658 F. App'x at 663. And in *Hammond v. The Bank of New York Mellon Corp.*, No. 08-6060, 2010 WL 2643307 (S.D.N.Y. June 25, 2010), the court, on summary judgment, found that the plaintiff could not provide evidence of mutual assent because, unlike here, "the parties had no relationship with each other." *Id.* at *11 ("[N]one of the named Plaintiffs had any direct dealings with Defendant; Plaintiffs dealt only with Defendant's institutional clients.").

As outlined in Sections I.B.-E. and II.B.3., *supra*, Plaintiff has adequately alleged actual damages as a result of Defendant's failure to protect Plaintiffs' and Class Members' PII.

D. Plaintiffs State A Claim For Unjust Enrichment.

Defendant asserts that Plaintiffs failed to allege the manner in which Defendant was unjustly enriched at Plaintiffs' expense. Defendant is mistaken. A plaintiff claiming unjust enrichment must demonstrate that "(1) the other party was enriched, (2) at that party's expense, and (3) that it is against equity and good conscience to permit the other party to retain what is sought to be recovered." *Georgia Malone & Co., Inc. v. Rieder*, 973 N.E.2d 743, 746 (N.Y. 2012). Plaintiffs properly allege unjust enrichment. *See* Compl. ¶¶ 90-97. Plaintiffs conferred their labor as a benefit upon Defendant, which Defendant accepted in exchange for the provision of wages, benefits, and reasonable security measures to secure the PII employees were required to provide as a part of their employment. *Id.* Rather than provide a reasonable level of security in accordance with industry standards that would have easily prevented the disclosures (*i.e.*, data security trainings, firewalls, and PII retention and destruction policies and procedures), *Id.* ¶ 93), Defendant instead knowingly and deliberately enriched itself with the cost savings it should have expended on data security while continuing to obtain the benefits conferred on it by employees' labor. *Id.* ¶¶ 92-96; *see Enslin*, 136 F. Supp. 3d at 676-78 (holding that the plaintiffs adequately stated a claim for restitution and unjust enrichment in a nearly identical, yet less egregious, employer data breach action); *cf. Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012) (holding that the plaintiffs alleged sufficient facts to allow unjust enrichment claim to survive in data breach action where the defendant allegedly failed to "pay the administrative costs of data management and security . . . to secure sensitive information, as can be seen from the data breach"). Thus, it would be against equity and good conscience to permit Defendant to retain the

benefits it derived in connection with its deficient to non-existent security measures and the Data Breach, while Plaintiffs continue to suffer as a result.¹⁴

E. Plaintiffs State A Claim For Violation of N.Y. LABOR LAW § 203-d.

Without the benefit of authority, or even argument, Defendant contends there is no private right of action under 203-d. Def.'s Mtn. 19-20. Not so. N.Y. LABOR LAW § 203-d is a statute intended to protect employees from the exact improper dissemination of PII as Plaintiffs allege. New York Courts hold that a private right of action exists under statutes designed to prevent specific injuries suffered by specific classes of persons, even where the statutory provision at issue provides for a specific enforcement mechanism by state officials or agencies. *See, e.g., Schwartz v. Torrenzano*, 16 N.Y.S.3d 697, 703 (N.Y. Sup. Ct. 2015) (private right of action where law included express state enforcement method). Therefore, while N.Y. LABOR LAW § 203-d does not expressly provide for a private right of action, § 203-d's statutory provisions and legislative intent require a finding that there is an implied private right of action.¹⁵

There is an implied private right of action under a statute that does not expressly reference such a right when "legislative intent to create such a right of action is fairly implied in the statutory provisions and their legislative history." *Maimonides Medical Center v. First United American Life Ins. Co.*, 981 N.Y.S.2d 739, 743 (N.Y. App. Div. 2014) (citing *Brian Hoxie's Painting Co. v. Cato-Meridian Cent. School Dist.*, 76 N.Y.2d 207, 211 (1990)). Thus, in the absence of an express prohibition, a private right of action may be implied when "(1) the plaintiff is one of the class for whose particular benefit the statute was enacted; (2) recognition of

¹⁴ Even assuming, *arguendo*, that Plaintiffs' unjust enrichment claim arises from the same alleged duties as their negligence and breach of implied contract claims, Defendant does not offer any grounds for claiming that the pleadings are deficient as filed, as Plaintiffs may plead such claims in the alternative. *See* Fed. R. Civ. P. 8(d)(2).

¹⁵ Defendant did not dispute its violations of N.Y. LABOR LAW § 203-d; rather, it repeated Plaintiffs' allegations and asserted that the statute "only permits enforcement by the commissioner." Def.'s Mtn. 19-20.

a private right of action would promote the legislative purpose of the statute; and (3) to do so would be consistent with the legislative scheme.” *AHA Sales, Inc. v. Creative Bath Prod., Inc.*, 867 N.Y.S.2d 169, 176-77 (2008) (citations omitted).

Plaintiffs satisfy all three factors. The statute is intended to strengthen New York’s identity theft laws by providing “important confidentiality safeguards *for employees*” and imposing duties on employers to safeguard “*employee personal identifying information . . .* including prohibiting employers from posting or displaying an employee’s social security number, or placing social security numbers in files with open access.” *See* Sponsors’ Mem., Bill Jacket, 2008 S.B. 8376, Ch. 279, at 7-9 (N.Y. 2008) (emphases added), Ex. 2 to Frei-Pearson Decl. Consequently, Plaintiffs are members of the class the statute was intended to benefit.

With respect to legislative purpose, “the New York Labor Law reflects a strong legislative policy aimed at redressing the power imbalance between employer and employee. Implying a right of action . . . would therefore comport with the purposes and policies underlying the Labor Law.” *Chu Chung v. New Silver Palace Restaurants, Inc.*, 272 F. Supp. 2d 314, 317 (S.D.N.Y. 2003) (quotations omitted) (collecting cases). Moreover, private enforcement will promote the legislative purpose of protecting employees’ PII because allowing private civil prosecution of unlawful conduct will foster increased employer accountability and will incentivize compliance. *See Ader v. Guzman*, 23 N.Y.S.3d 292, 295 (N.Y. App. Div. 2016) (holding that the threat of private enforcement will further ensure compliance).

Furthermore, a private right of action is entirely consistent with the legislative scheme. Indeed, where, as here, the Legislature delegated administrative enforcement of the statute, courts have consistently found that “a private right of action, in addition to administrative enforcement, is fully consistent with the legislative scheme” and therefore may be implied.

Maimonides, 981 N.Y.S.2d at 743; *accord Ader*, 23 N.Y.S.3d at 295 (holding that implied right of action is consistent with legislative scheme because threat of private action, in addition to designated administrative enforcement, would incentivize compliance); *Schwartz*, 16 N.Y.S.3d at 703 (holding that statutory assignment of enforcement authority “is not dispositive,” particularly “when a statute is not simply remedial in nature but is directed toward protecting . . . a particular class of individuals”) (collecting cases).¹⁶

New York courts are especially inclined to allow private citizens to maintain a cause of action despite statutory provision of administrative enforcement when the statute affords particular individuals rights and imposes affirmative duties on others. *Henry v. Isaac*, 632 N.Y.S.2d 169, 170 (1995) is directly on point. In *Henry*, the plaintiff brought a claim pursuant to Article 7 of New York’s Social Services Law and regulations promulgated thereunder. The defendant argued that the statute did not provide for a private right of action because it explicitly provided statutory and regulatory supervisory and enforcement authority to the Department of Social Services and the Attorney General. While the Appellate Division conceded that the supervisory and enforcement authorities granted “are indeed broad and comprehensive,” the Court rejected the defendant’s argument and held that the statute and regulations “afford [the plaintiffs] various rights and impose an affirmative duty [on the defendant],” such that a private right of action permitting individuals to seek redress would enhance the existing legislative scheme. *Henry*, 632 N.Y.S.2d at 193. Plaintiffs’ entitlement to a private right of action in is

¹⁶ See also *Doe v. Roe*, 599 N.Y.S.2d 350, 354 (1993) (permitting an implied private cause of action for disclosure of confidential information in violation of a public health statute because it was consistent with the three-factor test and “would merely provide an additional enforcement mechanism at the hands of those persons affected by a violation of that law and those whom the Legislature has deemed in need of protection”); *Maraia v. Orange Reg’l Med. Ctr.*, 882 N.Y.S.2d 287, 289-90 (2009) (holding that a private right of action is not inconsistent with the legislative scheme provided under the Labor Labor); *Gerel Corp. v. Prime Eastside Holdings, LLC*, 783 N.Y.S.2d 355, 360 (2004) (“That the Attorney General has standing to institute an action under General Obligations Law § 7-105 for a violation does not, in and of itself, defeat the existence of a private right of action.”).

more straightforward. Whereas the statute at issue in *Henry* related to the technical operation of adult care facilities, here the entire purposes of the statute is to protect employees' PII.

Ader v. Guzman is similarly persuasive. In *Ader*, the court found a private right of action under Southampton Town Code § 270 holding that “[a]lthough Town Code § 270 is intended to be enforced by designated Town officials and provides for penalties and fines, without the threat of recoupment of rent, aside from the possibility of administrative enforcement, there is no incentive for a landlord to obtain a license, which is an overriding concern of the Town.” *Ader*, 23 N.Y.S.3d at 295. Again, the same is true here except the rights implicated as it relates to Plaintiffs are even more personal and direct in nature.¹⁷

In addition, the legislative history of 203-d reflects no intent to foreclose private enforceability. Rather, the Legislature focused its efforts on providing specific protections to employees and their PII, and imposing affirmative duties on their employers. *See* Sponsors' Mem., Bill Jacket, 2008 S.B. 8376, Ch. 279, at 7-9 (N.Y. 2008), Ex. 2 to Frei-Pearson Decl. A private right of action simply provides victims with an additional enforcement mechanism that enhances the administrative mechanism and promotes the legislature's goals.

CONCLUSION

For the reasons set for above, Plaintiffs respectfully request that TransPerfect's Motion to Dismiss be denied in its entirety.

¹⁷ *See also Maimonides*, 981 N.Y.S.2d at 745 (finding that, where the statute “impose[s] specific duties upon insurers and create[s] rights in patients and health care providers, [it] thus militates in favor of the recognition of an implied private right of action to enforce such rights”); *Nat'l Convention Servs., L.L.C. v. Applied Underwriters Captive Risk Assurance Co., Inc.*, No. 15-07063, 2017 WL 945189, at *15 (S.D.N.Y. Mar. 9, 2017) (citations omitted) (finding an implied private right of action fully consonant with the legislative scheme where the statute contains mandatory language (“shall”) and determination of a violation “[does] not require any special agency expertise”); *Uhr v. East Greenbush Cent. School Dist.*, 94 N.Y.2d 32, 40-41 (1999) (finding that a private right of action would not be consistent with the legislative scheme where there was “persuasive evidence as to the Legislature's intent to immunize the school districts for both nonfeasance and misfeasance” liability, and because “[a]llowing a private right of action against the government as opposed to a private entity has direct and obvious financial consequences to the public”).

Respectfully Submitted,



Jeremiah Frei-Pearson
D. Greg Blankinship
Chantal Khalil
**FINKELSTEIN, BLANKINSHIP,
FREI-PEARSON & GARBER, LLP**
445 Hamilton Avenue, Suite 605
White Plains, New York 10601